

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

EB Docket No. 06-36

ANNUAL 47 C.F.R § 64.2009(e) CPNI CERTIFICATION

Annual 64.2009(e) CPNI Certification for 2007

Date filed: September 23, 2008

Name of company covered by this certification: BBG Communications, Inc.

Form 499 Filer ID: 820964

Name of signatory: **Rafael Galicot**

Title of signatory: **Vice President**

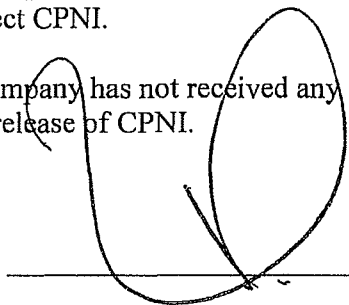
I, **Rafael Galicot**, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules, to the extent those procedures apply to the information we obtain in the provision of our services. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system or at the Commission) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



BBG COMMUNICATIONS, INC

STATEMENT OF CPNI PROCEDURES

BBG Communications, Inc. ("BBG") takes the protection of CPNI seriously. BBG has received legal counsel in this area and protects the confidentiality of its customers' information. BBG receives limited information from its customers and uses that information solely to perform the telecommunications services, for billing purposes and in response to legal process. It does not use this information for marketing purposes.

BBG provides international telecommunications services, including public telephony, calling card, long distance operator assistance, credit card processing, billing, collection and wireless telecommunications services. BBG processes casual-use voice services from European Union ("EU") telephone users making long distance calls from payphones and hotels. This process includes the collection of billing information and desired call destination from end users which eventually result in the creation of call detail records and include the date, time, duration, number dialed and billing number (the "Information"). The Information is collected from EU telephone equipment operators, and local and long distance carriers and is used by BBG for calculating commissions and reporting this information via a secured website to sales representatives and customers; otherwise the information is restricted to authorized personnel, technical staff and network administrators.

Duty to Protect CPNI

We recognize a duty to protect customer CPNI if we possess CPNI. To the extent we obtain CPNI, we may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

1. Administrative use: We may use CPNI to *initiate, render, bill and collect* for communications services.
2. Protection of carrier and third parties: We may use CPNI to protect the interests of our company, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.
3. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

Our Own Use Of CPNI

We do not use CPNI to market to customers. We do not share CPNI with any affiliates or other third parties for marketing purposes. BBG does not share or disclose the Information with affiliates or third parties unless required to do so by law.

An individual's name and credit card number are collected when calls are billed to a credit card, and BBG processes the payment and charges to the caller's credit card. Certain related entities in the EU have also contracted with BBG to provide telecommunications support services.

Authenticating Customers Before Disclosing CPNI

We understand that we are required to objectively determine that our customers are who they say they are before disclosing CPNI to them.

Telephone

We do not release *call detail information*, or information relating to the transmission of specific telephone calls over the telephone. Our carrier customers can only access this information through a secure, authenticated network.

In-Person Authentication

We do not release CPNI through in-person visits. Our carrier customers can only access this information through a secure, authenticated network.

Mail

If the customer requests CPNI through regular mail, or if the customer cannot comply with the authentication method above, we send the requested information to the customer's address of record only.

Online Access

We use strong cryptography and encryption techniques. For all web sites set up by BBG, 28 bit SSL encryption is enforced for all pages where customer information data is present. For all communications with external entities sending customer information data to BBG, strong encryption channels are set up, such as SSH, SSL, or SFTP. All BBG admin access to the web site machines uses SSH.

BBG does not permit wireless networks to transmit customer information data unless a SSL channel has first been established.

Training And Discipline

We have trained applicable employees regarding the company's CPNI policies. Employees will have an annual retraining to ensure that they understand the company's CPNI policies and any updates to those policies. New employees who will have access to CPNI will be trained when they join the company, and then attend the regularly-scheduled retraining sessions. Employees are subject to disciplinary action for failure to abide by our requirements.

Record-Keeping

We maintain records of discovered CPNI breaches, notifications to law enforcement regarding breaches, and any responses from law enforcement regarding those breaches, in our files for at least two (2) years.

Unauthorized Disclosure Of CPNI

We understand that we must report CPNI breaches to law enforcement no later than seven (7)

business days after determining the breach has occurred, by sending electronic notification through the link at <http://www.fcc.gov/eb/CPNI/> to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

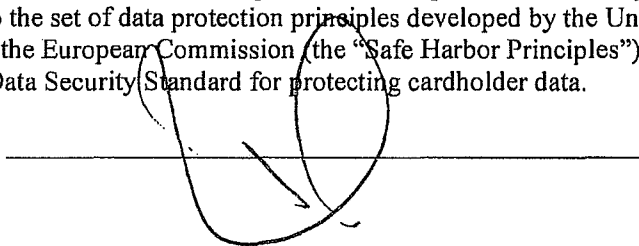
Records relating to such notifications are kept in accordance with our record-keeping policies. These records include: (i) the date we discovered the breach, (ii) the date we notified law enforcement, (iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

Additional Protections

BBG has established business procedures and policies to ensure protection of the Information. BBG adheres to the set of data protection principles developed by the United States Department of Commerce and the European Commission (the "Safe Harbor Principles") and adheres to the Payment Card Industry Data Security Standard for protecting cardholder data.

Signed

A handwritten signature, appearing to be "G. [unclear]", is written over a horizontal line. The signature is in dark ink and is somewhat stylized.